UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/500,370	07/28/2004	Jaakko Rajaniemi	800.0180.U1(US)	7601

29683 7590 05/11/2010
HARRINGTON & SMITH
4 RESEARCH DRIVE, Suite 202
SHELTON, CT 06484-6212

EXAMINER	
HOLLIDAY, JAIME MICHELE	
ART UNIT	PAPER NUMBER
2617	
MAIL DATE	DELIVERY MODE
05/11/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/500,370	RAJANIEMI, JAAKKO	
	Examiner	Art Unit	
	JAIME M. HOLLIDAY	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 January 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12,14-19,21,29-32,34,35,37,38,40-43,45-47 and 49-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12,14-19,21,29-32,34,35,37,38,40-43,45-47 and 49-51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on January 29, 2010 has been entered.

Response to Arguments

2. Applicant's arguments with respect to **claims 1-12, 14-19, 21, 29-32, 34, 35, 37, 38, 40-43, 45-47 and 49-51** have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. **Claims 1-5, 8, 9, 14, 16, 21, 29-32, 34, , 37, 38, 40, 42, 43, 46, 47, 50 and 51** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Boyle et al. (US 6,647,259 B1)** in view of **Lamb (6,085,083)**, and in further view of **Bui et al. (US 6,412,007 B1)**.

Consider **claim 1**, Boyle et al. clearly show and disclose a method, comprising: using an authorization and authentication profile associated with a user (HLR record for mobile unit [col. 3 lines 23-26]), including the authorization and authentication profile is sent from an authentication and authorization device located in a home network to a server node (home wireless system receives the registration and sends a profile of the mobile user to the visited wireless system [col. 3 lines 46-50]); and the authorization and authentication profile is stored at the server node (sends a profile of the mobile user to the visited wireless system; profile is obtained from the HLR record [col. 3 lines 46-50]).

However, Boyle et al. fail to specifically disclose that the profile allows the server node to authorize and authenticate directly.

In the same field of endeavor, Lamb clearly shows and discloses wherein the authorization and authentication profile contains information which allows the server node to authorize and authenticate the user directly without contacting the authentication and authorization device (each MSC communicating to an HLR has a corresponding MPCM file record in the MPCM file of the HLR; SUBS file **222** is the "subscribers' files" which store subscribers' profiles on a per subscriber basis; FRAUD--INFO segment of a subscriber's profile record indicates whether or not fraud protection (i.e., FP check) is authorized for this subscriber; The OPT7_IND field indicates whether the Visitor Location Register (VLR) serving this MSC can perform an authentication (AC) check [col. 2 line 61- col. 3 line 6, col. 4 lines 29- col. 5 line 10, lines 46-50).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to authorize fraud protection as taught by Lamb in the method of Boyle et al., in order to include fraud protection in the HLR (Lamb; abstract).

However, Boyle et al., as modified by Lamb, fail to specifically disclose authorization is verified when the number of simultaneous session is equal to a predetermined number.

In the same field of endeavor, Bui et al. clearly show and disclose wherein the authorization and authentication profile further contains information defining that the authentication and authorization device is to be contacted when a number of simultaneous sessions for the user is equal to a predetermined number (after determining the number of sessions that are currently established for a particular entity, the local DSC compares the number to a session threshold value, wherein the threshold identifies the maximum number of session allowed before SLOW LANE authorization is required; each DSC maintains its own local copy of the information maintained in the global database [fig. 2, col. 5 lines 36-50, line 60- col. 6 line 8, lines 12-22, col. 18 lines 45-53]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to perform an authentication after the number of currently established sessions reaches a maximum as taught by Bui et al. in the method of Boyle et al., as modified by Lamb, in order to control authorization and access to a system and/or its services.

Consider **claim 2**, the combination of Boyle et al. and Lamb, as modified by Bui et al., clearly shows and discloses the claimed invention **as applied to claim 1 above**, and in addition, Boyle et al. further disclose transferring said information from the authentication and authorization device to the server node in at least one of a signaling path for the service setup, a service event, and a registration (home wireless system receives the registration and sends a profile of the mobile user to the visited wireless system [col. 3 lines 46-50]).

Consider **claims 3 and 4**, the combination of Boyle et al. and Lamb, as modified by Bui et al., clearly shows and discloses the claimed invention as **applied to claim 1 above**, and in addition, Bui et al. further disclose wherein said information indicates, that at least one of the authentication and authorization needs to be verified; performing at least one of the authentication and the authorization of the user (wherein the threshold identifies the maximum number of session allowed before SLOW LANE authorization is required [fig. 2, col. 5 lines 36-50, line 60- col. 6 line 8, lines 12-22, col. 18 lines 45-53]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to perform an authentication after the number of currently established sessions reaches a maximum as taught by Bui et al. in the method of Boyle et al., as modified by Lamb, in order to control authorization and access to a system and/or its services.

Consider **claim 5**, the combination of Boyle et al. and Lamb, as modified by Bui et al., clearly shows and discloses the claimed invention **as applied to claim 4 above**,

and in addition, Bui et al. further disclose performing at least one of the authentication and the authorization of the user by using the authentication and authorization device (authoritative DSC determines whether the session should be allowed for the particular entity [col. 6 lines 13-55]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to perform an authentication by the authoritative DSC and not the local DSC as taught by Bui et al. in the method of Boyle et al., as modified by Lamb, in order to control authorization and access to a system and/or its services.

Consider **claim 7**, Boyle et al. clearly show and disclose using an authorization and authentication profile associated with a user (HLR record for mobile unit [col. 3 lines 23-26]), wherein the authorization and authentication profile is received from an authentication and authorization device located in a home network, wherein the authorization and authentication profile is stored in a server node (home wireless system receives the registration and sends a profile of the mobile user to the visited wireless system [col. 3 lines 46-50]).

However, Boyle et al. fail to specifically disclose that the profile allows the server node to authorize and authenticate directly.

In the same field of endeavor, Lamb clearly shows and discloses wherein the authorization and authentication profile contains information which allows the server node to authorize and authenticate the user directly without contacting the authentication and authorization device, and wherein the information further includes a condition that, when satisfied, determines that the authentication and authorization

device is to be contacted (each MSC communicating to an HLR has a corresponding MPCM file record in the MPCM file of the HLR; SUBS file **222** is the "subscribers' files" which store subscribers' profiles on a per subscriber basis; FRAUD--INFO segment of a subscriber's profile record indicates whether or not fraud protection (i.e., FP check) is authorized for this subscriber; The OPT7_IND field indicates whether the Visitor Location Register (VLR) serving this MSC can perform an authentication (AC) check [col. 2 line 61- col. 3 line 6, col. 4 lines 29- col. 5 line 10, lines 46-50).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to authorize fraud protection as taught by Lamb in the method of Boyle et al., in order to include fraud protection in the HLR (Lamb; abstract).

However, Boyle et al., as modified by Lamb, fail to specifically disclose authorization is verified when the number of simultaneous session is equal to a predetermined number.

In the same field of endeavor, Bui et al. clearly show and disclose providing access to a service responsive to said authorization and authentication profile, wherein the condition is that authentication and authorization is verified with the authentication and authorization device when a number of simultaneous sessions for the user is equal to a predetermined number (after determining the number of sessions that are currently established for a particular entity, the local DSC compares the number to a session threshold value, wherein the threshold identifies the maximum number of session allowed before SLOW LANE authorization is required; each DSC maintains its own local

copy of the information maintained in the global database [fig. 2, col. 5 lines 36-50, line 60- col. 6 line 8, lines 12-22, col. 18 lines 45-53]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to perform an authentication after the number of currently established sessions reaches a maximum as taught by Bui et al. in the method of Boyle et al., as modified by Lamb, in order to control authorization and access to a system and/or its services.

Consider **claim 8**, and **as applied to claim 7 above**, Boyle et al., as modified by Lamb, clearly shows and discloses the claimed invention except determining whether said condition is satisfied and providing access to said service without authorizing.

In the same field of endeavor, Bui et al. further disclose determining whether said condition is satisfied; and providing access to said service without authorizing and authenticating the user when said condition is not satisfied (the local DSC compares the number of sessions that are currently established for the particular entity with a "local" session threshold value that is maintained for the particular entity, based on the comparison, the local DSC determines whether it can authorize the session itself (FAST LANE); if the local DSC determines that it can authorize the session itself, it sends an authorization grant message back to the network access server without requesting authorization from the authoritative DSC [col. 6 lines 13-55]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to perform an authentication by the local DSC after comparison of simultaneous sessions as taught by Bui et al. in the method of Boyle et

al., as modified by Lamb, in order to control authorization and access to a system and/or its services.

Consider **claim 9**, and **as applied to claim 7 above**, Boyle et al., as modified by Lamb, clearly shows and discloses the claimed invention except determining whether said condition is satisfied; authorizing and authenticating the user when said condition is satisfied; and subsequent to authorizing and authenticating the user, providing access to said service when said authorizing indicates that the user is permitted access to said service.

In the same field of endeavor, Bui et al. disclose determining whether said condition is satisfied; authorizing and authenticating the user when said condition is satisfied; and subsequent to authorizing and authenticating the user, providing access to said service when said authorizing indicates that the user is permitted access to said service (the local DSC compares the number of sessions that are currently established for the particular entity with a "local" session threshold value that is maintained for the particular entity, based on the comparison, the local DSC determines whether it can authorize the session itself (FAST LANE); if the local DSC determines that it can authorize the session itself, it sends an authorization grant message back to the network access server without requesting authorization from the authoritative DSC [col. 6 lines 13-55]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to perform an authentication by the local DSC after comparison of simultaneous sessions as taught by Bui et al. in the method of Boyle et

al., as modified by Lamb, in order to control authorization and access to a system and/or its services.

Consider **claim 14**, and **as applied to claim 7 above**, Boyle et al., as modified by Lamb, clearly shows and discloses the claimed invention except generating a register message at said user equipment and transmitting said register message to a local server node of said communication system; determining whether a condition indicated by said an authorization and authentication profile is stored at said local server node is satisfied; generating an access message at said local server node indicating that access to said service is permitted; and transmitting said access message to said service provider node.

In the same field of endeavor, Bui et al. clearly show and disclose generating a register message at said user equipment and transmitting said register message to a local server node of said communication system; determining whether a condition indicated by said an authorization and authentication profile is stored at said local server node is satisfied; generating an access message at said local server node indicating that access to said service is permitted; and transmitting said access message to said service provider node (the local DSC compares the number of sessions that are currently established for the particular entity with a "local" session threshold value that is maintained for the particular entity, based on the comparison, the local DSC determines whether it can authorize the session itself (FAST LANE); if the local DSC determines that it can authorize the session itself, it sends an authorization grant message back to

the network access server without requesting authorization from the authoritative DSC [col. 6 lines 13-55]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to perform an authentication by the local DSC after comparison of simultaneous sessions as taught by Bui et al. in the method of Boyle et al., as modified by Lamb, in order to control authorization and access to a system and/or its services.

Consider **claim 16**, the combination of Boyle et al. and Lamb, as modified by Bui et al., clearly shows and discloses the claimed invention **as applied to claim 7 above**, and in addition, Bui et al. further disclose generating an invite message at said user equipment and transmitting said invite message to a local server node of said communication system; determining whether a condition indicated by an authorization and authentication profile stored at said local server node is satisfied; generating an access message at said local server node indicating that access to said service is permitted; and transmitting said access message to said service provider node (the local DSC compares the number of sessions that are currently established for the particular entity with a "local" session threshold value that is maintained for the particular entity, based on the comparison, the local DSC determines whether it can authorize the session itself (FAST LANE); if the local DSC determines that it can authorize the session itself, it sends an authorization grant message back to the network access server without requesting authorization from the authoritative DSC [col. 6 lines 13-55]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to perform an authentication by the local DSC after comparison of simultaneous sessions as taught by Bui et al. in the method of Boyle et al., as modified by Lamb, in order to control authorization and access to a system and/or its services.

Consider **claim 21**, Boyle et al. clearly show and disclose an apparatus, comprising: at least one interface configured to receive a message from a user terminal and to receive authorization and authentication profile associated with a user from an authentication authorization device located in a home network using an authorization and authentication profile associated with a user (mobile unit will register with the home wireless system; home wireless system receives the registration and sends a profile of the mobile user to the visited wireless system [col. 3 lines 23-50]); a memory configured to store the authorization and authentication profile associated with the user (sends a profile of the mobile user to the visited wireless system; profile is obtained from the HLR record [col. 3 lines 46-50]).

However, Boyle et al. fail to specifically disclose that the profile allows the server node to authorize and authenticate directly.

In the same field of endeavor, Lamb clearly shows and discloses a memory configured to store the authorization and authentication profile associated with the user, wherein the authorization and authentication profile contains information which allows the user to be authorized and authenticated directly with the apparatus without contacting the authorization and authentication device, and wherein the information

further includes a condition that, when satisfied, determines that the authentication and authorization device is to be contacted (each MSC communicating to an HLR has a corresponding MPCM file record in the MPCM file of the HLR; SUBS file **222** is the "subscribers' files" which store subscribers' profiles on a per subscriber basis; FRAUD--INFO segment of a subscriber's profile record indicates whether or not fraud protection (i.e., FP check) is authorized for this subscriber; The OPT7_IND field indicates whether the Visitor Location Register (VLR) serving this MSC can perform an authentication (AC) check [col. 2 line 61- col. 3 line 6, col. 4 lines 29- col. 5 line 10, lines 46-50).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to authorize fraud protection as taught by Lamb in the method of Boyle et al., in order to include fraud protection in the HLR (Lamb; abstract).

However, Boyle et al., as modified by Lamb, fail to specifically disclose authorization is verified when the number of simultaneous session is equal to a predetermined number.

In the same field of endeavor, Bui et al. clearly show and disclose the apparatus configured, in response to said authorization and authentication profile, to generate an access message to provide a user access to a service from a service provider node (if the local DSC determines that it can authorize the session itself, it sends an authorization grant message back to the network access server without requesting authorization from the authoritative DSC [col. 6 lines 13-55]), wherein the condition is that authorization and authentication is verified with the authentication and authorization device when a number of simultaneous sessions is equal to a

predetermined number (after determining the number of sessions that are currently established for a particular entity, the local DSC compares the number to a session threshold value, wherein the threshold identifies the maximum number of session allowed before SLOW LANE authorization is required; each DSC maintains its own local copy of the information maintained in the global database [fig. 2, col. 5 lines 36-50, line 60- col. 6 line 8, lines 12-22, col. 18 lines 45-53]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to perform an authentication after the number of currently established sessions reaches a maximum as taught by Bui et al. in the method of Boyle et al., as modified by Lamb, in order to control authorization and access to a system and/or its services.

Consider **claim 29**, Boyle et al. clearly show and disclose a method, comprising: storing an authorization and authentication profile, associated with a user, wherein the authorization and authentication profile is stored at a serving node in a serving network wherein the authorization and authentication profile is received from an authentication authorization device located in a home network (mobile unit will register with the home wireless system; home wireless system receives the registration and sends a profile of the mobile user to the visited wireless system; sends a profile of the mobile user to the visited wireless system; profile is obtained from the HLR record [col. 3 lines 23-50]).

However, Boyle et al. fail to specifically disclose that the profile allows the server node to authorize and authenticate directly.

In the same field of endeavor, Lamb clearly shows and discloses using said authorization and authentication profile at a serving node, wherein the authorization and authentication profile contains information which allows the user to be authorized and authenticated directly with the serving node in the serving network without contacting the authorization and authentication device, wherein the information further includes a condition that, when satisfied, determines that the authentication and authorization device is to be contacted (each MSC communicating to an HLR has a corresponding MPCM file record in the MPCM file of the HLR; SUBS file **222** is the "subscribers' files" which store subscribers' profiles on a per subscriber basis; FRAUD--INFO segment of a subscriber's profile record indicates whether or not fraud protection (i.e., FP check) is authorized for this subscriber; The OPT7_IND field indicates whether the Visitor Location Register (VLR) serving this MSC can perform an authentication (AC) check [col. 2 line 61- col. 3 line 6, col. 4 lines 29- col. 5 line 10, lines 46-50).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to authorize fraud protection as taught by Lamb in the method of Boyle et al., in order to include fraud protection in the HLR (Lamb; abstract).

However, Boyle et al., as modified by Lamb, fail to specifically disclose authorization is verified when the number of simultaneous session is equal to a predetermined number.

In the same field of endeavor, Bui et al. clearly show and disclose wherein the condition is that authorization and authentication is verified with the authentication and authorization device when a number of simultaneous sessions is equal to a

predetermined number (after determining the number of sessions that are currently established for a particular entity, the local DSC compares the number to a session threshold value, wherein the threshold identifies the maximum number of session allowed before SLOW LANE authorization is required; each DSC maintains its own local copy of the information maintained in the global database [fig. 2, col. 5 lines 36-50, line 60- col. 6 line 8, lines 12-22, col. 18 lines 45-53]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to perform an authentication after the number of currently established sessions reaches a maximum as taught by Bui et al. in the method of Boyle et al., as modified by Lamb, in order to control authorization and access to a system and/or its services.

Consider **claims 30, 31, 42, 46, 50 and 51**, Boyle et al. clearly show and disclose an apparatus [method; computer readable medium], comprising: an interface configured to receive a message from a user terminal; a receiver configured to receive data comprising an authorization and authentication profile from an authentication authorization device located in a home network (mobile unit will register with the home wireless system; home wireless system receives the registration and sends a profile of the mobile user to the visited wireless system [col. 3 lines 23-50]); a memory configured to store the authorization and authentication profile (sends a profile of the mobile user to the visited wireless system; profile is obtained from the HLR record [col. 3 lines 46-50]).

However, Boyle et al. fail to specifically disclose that the profile allows the server node to authorize and authenticate directly.

In the same field of endeavor, Lamb clearly shows and discloses a processor configured to use an authorization and authentication profile associated with said user terminal, wherein the authorization and authentication profile contains information which allows the user to be authenticated and authorized directly with the apparatus without contacting an authentication and authorization device located in a home network, and wherein the information further includes a condition that, when satisfied, determines that the authentication and authorization device is to be contacted (each MSC communicating to an HLR has a corresponding MPCM file record in the MPCM file of the HLR; SUBS file **222** is the "subscribers' files" which store subscribers' profiles on a per subscriber basis; FRAUD--INFO segment of a subscriber's profile record indicates whether or not fraud protection (i.e., FP check) is authorized for this subscriber; The OPT7_IND field indicates whether the Visitor Location Register (VLR) serving this MSC can perform an authentication (AC) check [col. 2 line 61- col. 3 line 6, col. 4 lines 29-col. 5 line 10, lines 46-50).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to authorize fraud protection as taught by Lamb in the method of Boyle et al., in order to include fraud protection in the HLR (Lamb; abstract).

However, Boyle et al., as modified by Lamb, fail to specifically disclose authorization is verified when the number of simultaneous session is equal to a predetermined number.

In the same field of endeavor, Bui et al. clearly show and disclose the processor configured to generate, in response to said authorization and authentication profile, an

access message to provide said user with access to a service from a service provider node (if the local DSC determines that it can authorize the session itself, it sends an authorization grant message back to the network access server without requesting authorization from the authoritative DSC [col. 6 lines 13-55]), wherein the condition is that authorization and authentication is verified with the authentication and authorization device when a number of simultaneous sessions is equal to a predetermined number (after determining the number of sessions that are currently established for a particular entity, the local DSC compares the number to a session threshold value, wherein the threshold identifies the maximum number of session allowed before SLOW LANE authorization is required; each DSC maintains its own local copy of the information maintained in the global database [fig. 2, col. 5 lines 36-50, line 60- col. 6 line 8, lines 12-22, col. 18 lines 45-53]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to perform an authentication after the number of currently established sessions reaches a maximum as taught by Bui et al. in the method of Boyle et al., as modified by Lamb, in order to control authorization and access to a system and/or its services.

Consider **claims 32, 38, 43 and 47**, the combination of Boyle et al. and Lamb, as modified by Bui et al., clearly shows and discloses the claimed invention **as applied to claims 30, 31, 42 and 46 above**, respectively, and in addition, Bui et al. further disclose a transmitter configured to transmit said access message to a service provider (the local DSC compares the number of sessions that are currently established for the particular

entity with a "local" session threshold value that is maintained for the particular entity, based on the comparison, the local DSC determines whether it can authorize the session itself (FAST LANE); if the local DSC determines that it can authorize the session itself, it sends an authorization grant message back to the network access server without requesting authorization from the authoritative DSC [col. 6 lines 13-55]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to perform an authentication by the local DSC after comparison of simultaneous sessions as taught by Bui et al. in the method of Boyle et al., as modified by Lamb, in order to control authorization and access to a system and/or its services.

Consider **claim 34 and 40**, the combination of Boyle et al. and Lamb, as modified by Bui et al., clearly shows and discloses the claimed invention **as applied to claims 30 and 31 above**, respectively, and in addition, Boyle et al. further disclose serving or proxy-call session control function node (feature control network includes control point, signal transfer points and a home location registry [col. 3 lines 13-28]).\

Consider **claim 37**, the combination of Boyle et al. and Lamb, as modified by Bui et al., clearly shows and discloses the claimed invention **as applied to claim 31 above**, and in addition, Boyle et al. further disclose storage configured to store the authorization and authentication profile (sends a profile of the mobile user to the visited wireless system; profile is obtained from the HLR record [col. 3 lines 46-50]).

5. **Claims 6, 10-12, 17 and 18** are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of **Boyle et al. (US 6,647,259 B1)** and **Lamb (6,085,083)**, in view of **Bui et al. (US 6,412,007 B1)**, and in further view of **Chavez et al. (US 6,591,102 B1)**.

Consider **claim 6**, and **as applied to claim 4 above**, the combination of Boyle et al. and Lamb, as modified by Bui et al., clearly shows and discloses the claimed invention except authenticating or authorizing the user when the required parameters are available.

In the same field of endeavor, Chavez et al. further discloses where at least one of the authentication and the authorization of the user is performed in server node if the required parameters are available (the base station determines whether the authentication information is stored in the memory, and if it is, the base station reads the authentication information and performs normal authentication [col. 5 lines 25-60]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to perform authentication if the base station has the authentication information is stored in its memory as taught by Chavez et al. in the method of Boyle et al. and Lamb, as modified by Bui et al., in order to control authorization and access to a system and/or its services.

Consider **claim 10**, and **as applied to claim 7 above**, the combination of Boyle et al. and Lamb, as modified by Bui et al., clearly shows and discloses the claimed invention except determining the condition when the call session is initiated.

In the same field of endeavor, Chavez et al. further disclose determining whether said condition is satisfied when a call session between said user and said service provider node is initiated (if the request is an incoming service request, which could be an outgoing service request including a telephone number requesting a call, the base station reads the authentication information from the incoming service request, the information may or may not stored in memory for future use, if it is normal authentication is performed, if it isn't the base station transmits a request for authentication information [col. 5 lines 10-60]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to perform authentication when an incoming service request is received as taught by Chavez et al. in the method of Boyle et al. and Lamb, as modified by Bui et al., in order to control authorization and access to a system and/or its services.

Consider **claim 11**, and **as applied to claim 7 above**, the combination of Boyle et al. and Lamb, as modified by Bui et al., clearly shows and discloses the claimed invention except determining the condition exists during a call session.

In the same field of endeavor, Chavez et al. further disclose determining from the authorization and authentication profile associated with said user if said condition exists during a call session between said user equipment and said service provider node (if the request is an incoming service request, which could be an outgoing service request including a telephone number requesting a call, the base station reads the authentication information from the incoming service request, the information may or

may not stored in memory for future use, if it is normal authentication is performed, if it isn't the base station transmits a request for authentication information [col. 5 lines 10-60]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to perform authentication when a telephone number requesting a call as taught by Chavez et al. in the method of Boyle et al. and Lamb, as modified by Bui et al., in order to control authorization and access to a system and/or its services.

Consider **claim 12**, and **as applied to claim 7 above**, the combination of Boyle et al. and Lamb, as modified by Bui et al., clearly shows and discloses the claimed invention except the profile indicates that access is permitted without determination of the condition.

In the same field of endeavor, Chavez et al. further disclose determining from the authorization and authentication profile associated with said user if said condition exists during a call session between said user equipment and said service provider node (if the request is an incoming service request, which could be an outgoing service request including a telephone number requesting a call, the base station reads the authentication information from the incoming service request, the information may or may not stored in memory for future use, if it is normal authentication is performed, if it isn't the base station transmits a request for authentication information [col. 5 lines 10-60]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to perform authentication the base station reads the authentication information stored in its memory as taught by Chavez et al. in the method of Boyle et al. and Lamb, as modified by Bui et al., in order to control authorization and access to a system and/or its services.

Consider **claims 17 and 18**, and **as applied to claim 7 above**, the combination of Boyle et al. and Lamb, as modified by Bui et al., clearly shows and discloses the claimed invention except that the access is explicitly authorized and authenticated for service.

In the same field of endeavor, Chavez et al. further disclose information indicates whether said user is authorized to access said service; information indicates whether said user is authenticated to access said service (if a the service information is not stored in memory from a previous request for the service information, a request is sent to the service provider which has a database that stores all the services a mobile is allowed to receive [col. 6 lines 20-35, col. 1 lines 35-60]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to determine the services that a mobile is allowed to receive as taught by Chavez et al. in the method of Boyle et al. and Lamb, as modified by Bui et al., in order to control authorization and access to a system and/or its services.

6. **Claims 15, 35, 41, 45 and 49** are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of **Boyle et al. (US 6,647,259 B1)** and **Lamb**

(6,085,083), in view of **Bui et al. (US 6,412,007 B1)**, and in further view of **Basilier et al. (6,728,536)**.

Consider **claim 15**, and **as applied to claim 14 above**, the combination of Boyle et al. and Lamb, as modified by Bui et al., clearly show and disclose the claimed invention, except that the information is specifically requested prior to storing the specific record and is transferred from the AAA-H in response.

In the same field of endeavor, Basilier et al. clearly show and disclose prior to said storing said authorization and authentication profile, generating a request message at said local server node and transmitting said request message to the authentication and authorization device; and receiving data comprising said authorization and authentication profile from said authentication and authorization device responsive to said request message (a user wished to use the mobile terminal in the visited network, and registers in the visited network. The ACS/VLR assembles a registration and/or authentication message, and sends it to the AAA-F. The AAA-F uses a NAI to locate the appropriate AAA-H, and route the message to the appropriate HLR. The HLR validates or denies the registration request, and generates an appropriate response message, which is transmitted to the visited network [fig.2 b., col. 4 line 52- col. 5 line 25, col. 6 lines 15-30]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to authenticate a user by communicating with the home network (HLR, AAA-H) as taught by Basilier et al. in the method of Boyle et al.

and Lamb, as modified by Bui et al., in order to include fraud protection in the HLR (Lamb; abstract).

Consider **claims 35, 41, 45 and 49**, and **as applied to claims 30, 31, 42 and 46 above**, respectively, the combination of Boyle et al. and Lamb, as modified by Bui et al., clearly show and disclose the claimed invention, except that the information included in the specific record specifically includes a first field for identifying the user and a second field to identify when to authenticate at the AAA-H.

In the same field of endeavor, Basilier et al. clearly show and disclose wherein said authorization and authentication profile comprises a first data field identifying said user and a second data field determining when at least one of authentication and authorization of said user is required in order to access said service (user wished to use the mobile terminal in the visited network, and registers in the visited network. The ACS/VLR assembles a registration and/or authentication message, and sends it to the AAA-F. The AAA-F uses a NAI, or the significant digits of the IMSI, to locate the appropriate AAA-H, and route the message to the appropriate HLR. The HLR validates or denies the registration request, and generates an appropriate response message, which is transmitted to the visited network [fig.2 b., col. 4 line 52- col. 5 line 25, col. 6 lines 15-30]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to authenticate a user by communicating with the home network (HLR, AAA-H) as taught by Basilier et al. in the method of Boyle et al.

and Lamb, as modified by Bui et al., in order to include fraud protection in the HLR (Lamb; abstract).

7. **Claim 19** is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of **Boyle et al. (US 6,647,259 B1)** and **Lamb (6,085,083)**, in view of **Bui et al. (US 6,412,007 B1)**, and in further view of **Wright (US 6,957,061 B1)**.

Consider **claim 19**, and **as applied to claim 7 above**, the combination of Boyle et al. and Lamb, as modified by Bui et al., clearly show and disclose the claimed invention except determining the frequency of performing authentication/authorization.

In the same field of endeavor, Wright clearly shows and discloses condition determines a frequency at which said user is to be at least one of authorized or authenticated during a call session between a user equipment and said service provider node (the user equipment can allow the authentication vector to be used for a predetermined time period, number of calls or total call duration. Before requesting service, the user equipment determined whether the authentication vector should still be valid and issues with the KSI given by the serving network or a special KSI, which forces the serving network to request a new authentication vector when the next service request is made [col. 3 lines 56-67]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to authenticate a user who has been previously authenticated depending on a predetermined set time as taught by Wright in the method

of Chavez et al. and Lamb, as modified by Bui et al., in order to provide maximum security for the home operator (Wright; col. 4 lines 3-4).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAIME M. HOLLIDAY whose telephone number is (571)272-8618. The examiner can normally be reached on Monday through Friday 7:30am to 4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Charles Appiah can be reached on (571) 272-7904. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Jaime M Holliday/
Examiner, Art Unit 2617

/Charles N. Appiah/
Supervisory Patent Examiner, Art Unit 2617